Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Segundo semestre 2023

PRÁCTICO 5: CONGRUENCIAS

Ejercicio 1. Probar que la relación de congruencia módulo m es una relación de equivalencia.

Ejercicio 2. Sea m un entero fijo y suponga que $a \equiv b \pmod{m}$. Probar las siguientes propiedades:

a. $\lambda a \equiv \lambda b \pmod{m}$, para todo $\lambda \in \mathbb{Z}$.

b. $a^n \equiv b^n \pmod{m}$ para todo $n \in \mathbb{N}$.

c. si $p(x)$ es un polinomio con coeficientes enteros, entonces $p(a) \equiv p(b) \pmod{m}$.

Ejercicio 3. Probar que $a \equiv b \pmod{m}$ si y solo si $a \equiv b+mi \pmod{mh}$ para algún i tal que: $0 \leq i < h$.

Ejercicio 4.

a. Si $a \equiv 22 \pmod{14}$, hallar el resto de dividir a a por 2, por 7 y por 14.

b. Si $a \equiv 13 \pmod{5}$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

c. Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\displaystyle\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

Ejercicio 5.

a. Probar que si a y b son enteros y p un número primo entonces $(a+b)^p \equiv a^p + b^p \pmod{p}$.
¿Vale el resultado si p no es primo?

b. Probar (por inducción) el Teorema de Fermat: $a^p \equiv a \pmod{p}$, para todo a entero y todo primo p.

Ejercicio 6. Probar lo siguiente:

a. La ecuación $x^2 - 1 \equiv 0 \pmod{7}$ tiene exactamente 2 soluciones distintas.

b. La ecuación $x^2 - 1 \equiv 0 \pmod{35}$ tiene al menos 4 soluciones distintas. Probar además que son las únicas.

Ejercicio 7. Sea $n \in \mathbb{N}$ cuya representación en base 10 es $a_k a_{k-1} \cdots a_2 a_1 a_0$.

a. Probar que $n \equiv 2a_1 + a_0 \pmod{4}$.

b. Probar que $n \equiv 4a_2 + 2a_1 + a_0 \pmod{8}$.

c. Proponer una generalización del resultado para congruencia módulo 2^i, con $i < k$. Probar esta generalización, o refutarla mediante un contraejemplo.

Ejercicio 8.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$, para todo $n \in \mathbb{N}$.

b. Enunciar y probar un criterio de divisibilidad entre 11.

c. Hallar el dígito d, de modo que el número $2d653874$ sea múltiplo de 11.

Ejercicio 9.

a. Probar que 2 es invertible módulo n si y solamente si n es impar. En tal caso, hallar el inverso.

b. Resolver la ecuación $2x + 1 \equiv 0 \pmod{69}$.

Ejercicio 10.

a. Determinar el último dígito de 3^{55}.

b. Hallar el resto de la división de 12^{1257} entre 5.

c. Hallar $71^{10} \pmod{141}$.

Ejercicio 11. El número de la cédula uruguaya tiene la forma $x_1x_2 \dots x_7$-x_8; donde cada $x_i,\ i = 1, 2 \dots 8$, es un dígito de 0 a 9. El dígito verificador x_8 se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{7} a_i \cdot x_i,$$

donde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 9, 8, 7, 6, 3, 4)$. Entonces x_8 es: $r \equiv -c \pmod{10},\ 0 \leq r < 10$.

a. Verificar que el dígito verificador de su cédula se obtiene mediante la fórmula dada arriba.

b. Investigar si el dígito verificador detecta el error de copiar mal un dígito (de los primeros 7).

c. Probar que el dígito verificador detecta el error de intercambiar dos dígitos consecutivos de los $x_1, x_2, \dots, x_7$ (en el sentido del ejercicio anterior).

d. Escribir un programa para comprobar si una secuencia de 8 dígitos es un número de cédula o no.

Ejercicio 12. Resolver cada una de las congruencias siguientes:

a. $3x \equiv 7 \pmod{16}$.

b. $2x + 8 \equiv 5 \pmod{33}$.

c. $3x+9 \equiv 8x+61 \pmod{64}$.

d. $6x - 1 \equiv 5 \pmod{12}$.

e. $9x + 3 \equiv 5 \pmod{18}$.

Ejercicio 13.

a. Probar que para todo $a \in \mathbb{Z}$ se cumple que

$$a^2 \equiv 0 \pmod{4} \qquad \text{o} \qquad a^2 \equiv 1 \pmod{4}.$$

b. Muestre que el número 342634535100234547254362 2 no es cuadrado perfecto ni cubo perfecto. Sugerencia: para la 1a parte use congruencia módulo 4, y para la 2a use congruencia módulo 9.

c. Probar que ningún número de la sucesión $a_1 = 11,\ a_2 = 111,\ a_3 = 1111,\ a_4 = 11111, \dots$ es un cuadrado perfecto.

Ejercicio 14. Sea $p(x)$ un polinomio con coeficientes enteros, tal que: $p(0) = 1$, $p(1) = 2$ y $p(2) = 5$. Probar que $p(x)$ no tiene raíces enteras.